PAT-NO: JP02004199249A

DOCUMENT-IDENTIFIER: JP 2004199249 A

TITLE: IC CARD

PUBN-DATE: July 15, 2004

INVENTOR-INFORMATION:

NAME	COUNTRY
NANBU, KEIICHI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
MATSUSHITA ELECTRIC IND CO LTD	N/A

APPL-NO: JP2002365089

APPL-DATE: December 17, 2002

INT-CL (IPC): **G06K019/073**, **G06F012/14**

ABSTRACT:

PROBLEM TO BE SOLVED: To make it difficult to analyze current consumption without lengthening an actual processing time in a contact type IC card to which a power is supplied from the outside.

SOLUTION: An IC card 21 is provided with a **random number generator as a power supply** current control circuit 24 and a breeder circuit for making current flow based on random numbers generated by the **random number generator**. Thus, it is difficult to analyze the change of the actual current consumption of an IC card logic part 10 because of current by the **random number generation circuit from power supply** current, and the privacy of the IC card 21 is protected. Since current is changed by random numbers, and it is not necessary to lengthen an actual processing time.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-199249
(P2004-199249A)
(43)公開日　平成16年7月15日(2004.7.15)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 19/073	G06K 19/00	P	5B017
G06F 12/14	G06F 12/14	320A	5B035

審査請求 未請求　請求項の数 6　OL　（全 10 頁）

(21)出願番号　特願2002-365089(P2002-365089)
(22)出願日　平成14年12月17日(2002.12.17)

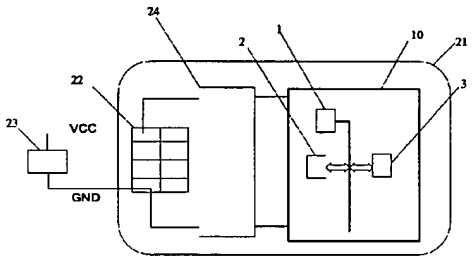
(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100099254
弁理士　役　昌明
(74)代理人　100100918
弁理士　大橋　公治
(74)代理人　100105485
弁理士　平野　雅典
(74)代理人　100108729
弁理士　林　紘樹
(72)発明者　南部　啓一
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

Fターム(参考)　5B017 AA03　BB03　CA14

最終頁に続く

(54)【発明の名称】ＩＣカード

(57)【要約】
【課題】外部から電源を供給する接触式のＩＣカードにおいて、実質の処理時間を長くすることなく、消費電流の解析を困難にする。
【解決手段】ＩＣカード21に、電源電流制御回路24として、乱数発生器と、乱数発生器で発生した乱数に基づいて電流を流すブリーダ回路とを設ける。乱数発生回路による電流のために、ＩＣカードロジック部10の実際の消費電流の変化を、電源電流から解析することが難しくなり、ＩＣカード21の機密を保護することができる。乱数で電流を変化させるので、実質的な処理時間を長くすることはない。
【選択図】　図１



【特許請求の範囲】
【請求項１】
外部から電源の供給を受けて動作するＩＣカードにおいて、前記電源で動作するＩＣカードロジック部と、前記ＩＣカードロジック部により制御される乱数発生器と、前記乱数発生器で発生した乱数に基づいて電流を流すブリーダ回路とを具備することを特徴とするＩＣカード。
【請求項２】
前記乱数発生器は、サブＣＰＵを用いた乱数発生器であることを特徴とする請求項１記載のＩＣカード。
【請求項３】
任意の時間に乱数を発生させるように、前記乱数発生器を制御する回路を備えたことを特徴とする請求項１または２記載のＩＣカード。
【請求項４】
乱数の種類を変化させるように、前記乱数発生器を制御する回路を備えたことを特徴とする請求項１または２記載のＩＣカード。
【請求項５】
任意の時間に乱数を変化させるように、前記乱数発生器を制御する回路を備えたことを特徴とする請求項１または２記載のＩＣカード。
【請求項６】
前記ブリーダ回路に流す電流を、実消費電流に応じて減少させる回路を備えたことを特徴とする請求項５記載のＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ＩＣカードに関し、特に、消費電流の解析攻撃に対するセキュリティを高めたＩＣカードに関する。
【０００２】
【従来の技術】
外部から電源を供給するタイプのＩＣカードは、リーダライタから電源の供給を受けて動作する。ＩＣカードは、リーダライタからの指示に従って、リーダライタとの間でデータの転送を行う。ＩＣカード用チップを構成しているＣＭＯＳ回路は、状態が変化する時に電流が流れるため、消費電流を観測すれば、ＩＣカード用チップ中の動作がある程度分かる。ＩＣカードは、ＩＤカードやマネーカードのように、内部に秘密データを保持して使われることが多いため、ＩＣカードがデータ処理を行っている時の消費電流を観測して解析することにより、秘密データの内容が推定できてしまう。これを避けるために、ＩＣデータの消費電流を解析しても、内部処理の状態を推測できないようにしたＩＣカードが提案されている。このような従来のＩＣカードとしては、特許文献１～３に開示されたものがある。
【０００３】
特許文献１に開示された「ＩＣカード」は、データ処理手順のタイミングを変化させる手段を設けることより、消費電流を測定しても、内部処理に依存するデータが得られないようにして、ＩＣカードの機密保護を図るものである。このＩＣカードには、データ処理装置と、データ処理手順が書き込まれたＲＯＭが内蔵されている。また、ＩＣカードの外部端子が、リードライト装置と電気的に接続されることによって、動作電圧が供給される。さらに、データ処理装置によるデータ処理手順のタイミングを変化させる手段が設けられている。このため、毎回、暗号処理の手順やタイミングが変わり、時間軸でみた場合の消費電流波形が変化する。したがって、電流波形を時間軸上で比較するというデータ依存性の解析が実質的に不可能になるので、機密保護ができる。
【０００４】
特許文献２に開示された「ＩＣカードと半導体集積回路装置」は、機密保護の強化を実現

したＩＣカードと半導体集積回路装置である。ＩＣカードの外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、データの入出力動作が行われる。ＩＣカードのＲＯＭには、データ処理装置によるデータ処理手順が書き込まれている。ＲＯＭに書き込まれたデータ処理手順に従って、データの入出力動作が行われる。図７に示すように、乱数発生回路70と偽電流発生回路71を設け、リードライト装置や外部装置との間でのデータの入出力動作に伴う内部回路動作と無関係で、かつ不規則性の電流値にされた電流を発生して、動作電圧が供給される電源端子に流す。

【０００５】

特許文献３に開示された「半導体集積回路装置」は、半導体集積回路装置自身の過渡的な動作電流を抑制し、半導体集積回路装置自身の発生するノイズを抑制するとともに、ＩＣカードの最重要課題でもある耐タンパー性の向上を図るものである。図８に示すように、本来機能の回路である主回路部81の動作電流を、動作電流検出回路部82で検出する。電流補償回路部83で、主回路部81の動作電流と逆位相の補償電流を流し、半導体集積回路装置80の同一チップの内部で合成することで、過渡的な動作電流を抑制する。

【０００６】

【特許文献１】

特開2000-259799号公報

【特許文献２】

特開2000-259784号公報

【特許文献３】

特開2000-164810号公報

【０００７】

【発明が解決しようとする課題】

しかしながら、従来のＩＣカードでは、ダミーの命令やデータを挿入するため、実質的な処理時間が長くなるという問題がある。

【０００８】

本発明の目的は、従来の問題を解決して、実質的な処理時間を長くすることなく、消費電流の解析を不可能にしてＩＣカードの機密を保護することである。

【０００９】

【課題を解決するための手段】

上記の課題を解決するために、本発明では、外部から電源の供給を受けて動作するＩＣカードにおいて、電源で動作するＩＣカードロジック部と、ＩＣカードロジック部により制御される乱数発生器と、乱数発生器で発生した乱数に基づいて電流を流すブリーダ回路とを具備する構成とした。

【００１０】

このように構成したことにより、乱数発生回路による電流のために、実際の電源電流の変化による解析が難しくなり、ＩＣカードの機密を保護することができる。

【００１１】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【００１２】

（第１の実施の形態）

本発明の第１の実施の形態は、乱数発生器で発生した乱数に基づいてダミー電流を流すＩＣカードである。

【００１３】

図１は、本発明の第１の実施の形態におけるＩＣカードの構成を示す概念図である。図１において、ＣＰＵ１は、ＩＣカードのデータを処理する演算回路である。ＲＯＭ２は、プログラムや固定データを格納したメモリである。ＲＡＭ３は、変更可能なデータを保持する不揮発性メモリである。ＩＣカードロジック部10は、ＣＰＵ１、ＲＯＭ２、ＲＡＭ３を含む論理回路部である。ＩＣカード21は、外部から電源を供給する接触式のＩＣカードで

ある。接触コネクタ22は、リーダライタとＩＣカード21とを接続する電極である。外部電源23は、電源を供給する手段である。電源電流制御回路24は、消費電流をランダムに変化させる回路である。

【００１４】

図２は、本発明の第１の実施の形態におけるＩＣカードの電源電流制御回路24に相当する回路を示す詳細図である。図１の構成と同じ構成については同一番号を付して、その説明を省略する。図２において、抵抗31は、ブリーダ用の抵抗である。トランジスタ32は、ダミー電流を流す回路であるブリーダの電流を制御する素子である。抵抗31とトランジスタ32で、ブリーダ(bleeder)回路を構成している。抵抗33は、ベース抵抗である。オペアンプ34は、乱数に応じた電圧でトランジスタ32に電流を流すように電圧を変換する回路である。抵抗35、抵抗36、抵抗37、抵抗38は、乱数を電圧に変換する素子である。乱数発生回路41は、適当な乱数を発生する回路である。乱数発生回路41は、サブＣＰＵで構成してもよい。

【００１５】

上記のように構成された本発明の第１の実施の形態におけるＩＣカードの動作を説明する。最初に、図１を参照しながら、ＩＣカードの機能の概略を説明する。外部電源23より、接触コネクタ22を経由し、電源電流制御回路24を通って、ＩＣカードロジック部10へ電源が供給される。ＣＰＵ１は、接触コネクタ22から入力される外部からの指示などに応じて、ＲＯＭ２に格納されたプログラムや固定データに基づき、ＲＡＭ３を参照しながら、ＩＣカードのデータを処理する。ＣＰＵ１の処理結果を、ＲＡＭ３に格納したり、接触コネクタ22を経由して外部に出力したりする。ＩＣカード21の基本的な機能は、従来のものと同様であるので、詳しい説明は省略する。電源電流制御回路24は、消費電流をランダムに変化させて、ＩＣカードロジック部10の消費電流をマスクする。

【００１６】

図２を参照しながら、電源電流制御回路24の動作を説明する。外部電源23より、接触コネクタ22を経由し、電源が供給されると、乱数発生回路41は動作開始する。乱数発生回路41の出力ポートＡ、Ｂ、Ｃは、抵抗36、抵抗37、抵抗38を介して、オペアンプ34に接続されている。出力ポートＡ、Ｂ、Ｃからは、乱数に応じたアナログ電圧が出力される。アナログ電圧は、抵抗35、抵抗36、抵抗37、抵抗38で合成され、適度な増幅度のオペアンプ34で増幅される。オペアンプ34の出力電圧は、抵抗33を介してトランジスタ32のベースに印加される。それにより、抵抗31を通してダミー電流が流れる。この抵抗31を流れる電流は、乱数発生回路41の乱数により逐次変化する。乱数発生回路41は、熱雑音を利用して乱数を発生する手段でもよいし、Ｍ系列信号を利用して擬似乱数を発生する手段でもよい。擬似乱数を発生する場合の初期値は、固定でもよいし、時計から時刻信号を得て初期値として利用してもよい。

【００１７】

上述の構成により、外部から検出される消費電流は、ＲＯＭ２、ＲＡＭ３のメモリをリード／ライトすることとは関係無しに変化するので、電流解析が難しくなり、セキュリティ確保が可能となる。

【００１８】

上記のように、本発明の第１の実施の形態では、ＩＣカードを、乱数発生器で発生した乱数に基づいてダミー電流を流す構成としたので、ＲＯＭ２やＲＡＭ３などのメモリのリード／ライト電流を解析することが困難になる。

【００１９】

（第２の実施の形態）

本発明の第２の実施の形態は、乱数発生器を制御して、任意の時間に乱数を発生させるようにしたＩＣカードである。

【００２０】

図３は、本発明の第２の実施の形態におけるＩＣカードの電源電流制御回路24に相当する回路を示す詳細図である。図１の構成と同じ構成については同一番号を付して、その説明

を省略する。図３において、第１出力ポート11は、ＩＣカードロジック部10に設けた出力ポートである。入力回路ポートＥＮは、乱数発生回路41の動作を制御する入力ポートである。乱数発生回路41は、サブＣＰＵで構成してもよい。

【００２１】

上記のように構成された本発明の第２の実施の形態におけるＩＣカードの動作を説明する。ＩＣカードロジック部10の第１出力ポート11を、乱数発生回路41の入力回路ポートＥＮに接続する。外部電源23より接触コネクタ22を経由し電源電流制御回路24を通って、ＩＣカードロジック部10へ電源が供給される。外部電源23より接触コネクタ22を経由し電源が供給されると、ＩＣカードロジック部10は動作する。ＩＣカードロジック部で、第１出力ポート11をＯＮすると、乱数発生回路の入力ポートＥＮはアクティブになり、乱数発生回路41は動作を開始する。その後の動作は、第１の実施の形態と同じである。

【００２２】

ＩＣカードロジック部10が、第１出力ポート11からの信号で、乱数発生回路41の入力ポートＥＮを制御することにより、乱数発生回路41が不要なとき、例えば、セキュリティが不要な通信時には乱数発生は不要であるから、乱数発生回路41の動作を中止することにより、消費電流の削減ができる。

【００２３】

上記のように、本発明の第２の実施の形態では、ＩＣカードを、乱数発生器を制御して、任意の時間に乱数を発生させるように構成したので、消費電流を削減できる。

【００２４】

（第３の実施の形態）

本発明の第３の実施の形態は、乱数発生器の初期値を変更可能にして、任意の乱数を発生させるようにしたＩＣカードである。

【００２５】

図４は、本発明の第３の実施の形態におけるＩＣカードの電源電流制御回路24に相当する回路を示す詳細図である。図１の構成と同じ構成については同一番号を付して、その説明を省略する。図４において、第２出力ポート12、第３出力ポート13、第４出力ポート14は、ＩＣカードロジック部10に設けた出力ポートである。入力ポートＤ、Ｅ、Ｆは、乱数発生回路41の初期値を選択できる入力ポートである。乱数発生回路41は、サブＣＰＵで構成してもよい。

【００２６】

上記のように構成された本発明の第３の実施の形態におけるＩＣカードの動作を説明する。ＩＣカードロジック部10の第２出力ポート12は、乱数発生回路41の入力回路ポートＤに接続され、同様に第３出力ポート13は入力ポートＥに接続され、第４出力ポート14は入力ポートＦに接続される。外部電源23より接触コネクタ22を経由し電源が供給されると、乱数発生回路41は動作開始する。ＩＣカードロジック部10の第２出力ポート12、第３出力ポート13、第４出力ポート14を任意に設定することにより、乱数発生回路41の初期値を任意に設定することができる。その後の動作は、第１の実施の形態と同じである。

【００２７】

乱数発生回路10の初期値を変更することにより、ＩＣカードの異なるアプリケーション毎に乱数を変更できるので、より一層電流解析が難しくなり、セキュリティ確保が確実にできる。

【００２８】

上記のように、本発明の第３の実施の形態では、ＩＣカードを、乱数発生器の初期値を変更可能にして、任意の乱数を発生させるように構成したので、メモリのリード／ライト電流を解析することが、一層困難になる。

【００２９】

（第４の実施の形態）

本発明の第４の実施の形態は、任意の時間に乱数を変化させるように、乱数発生器を制御するＩＣカードである。

【００３０】
図５は、本発明の第４の実施の形態におけるＩＣカードの電源電流制御回路24に相当する回路を示す詳細図である。図１の構成と同じ構成については同一番号を付して、その説明を省略する。図５において、第１出力ポート11は、ＩＣカードロジック部10に設けた出力ポートである。入力回路ポートＥＮは、乱数発生回路41の動作を制御する入力ポートである。第２出力ポート12、第3出力ポート13、第４出力ポート14は、ＩＣカードロジック部10に設けた出力ポートである。入力ポートＤ、Ｅ、Ｆは、乱数発生回路41の初期値を選択できる入力ポートである。乱数発生回路41は、サブＣＰＵで構成してもよい。
【００３１】
上記のように構成された本発明の第４の実施の形態におけるＩＣカードの動作を説明する。ＩＣカードロジック部10で、第１出力ポート11をＯＮすると、乱数発生回路41の入力ポートＥＮはアクティブになり、乱数発生回路41は動作を開始する。さらに、ＩＣカードロジック部10の第２出力ポート12、第３出力ポート13、第４出力ポート14を、任意に設定することにより、乱数発生回路41の初期値を設定できる。その後の動作は、第１の実施の形態と同じである。
【００３２】
乱数発生回路41に入力ポートＥＮを設け、ＩＣカードロジック部10に第１出力ポート11を設けることにより、例えば、セキュリティが不要な通信時のように、乱数発生が不要なとき、乱数発生回路41の動作を中止することができ、消費電流を削減できる。さらに、乱数発生回路10の初期値が変更できるので、ＩＣカードの異なるアプリケーション毎に乱数を変更でき、より一層電流解析が難しくなり、セキュリティ確保が可能となる。任意のタイミングで乱数発生回路10を動作させ、任意のタイミングで初期値を変更できるので、柔軟に乱数を発生することができる。
【００３３】
上記のように、本発明の第４の実施の形態では、ＩＣカードを、任意の時間に乱数を変化させるように、乱数発生器を制御する構成としたので、メモリのリード／ライト電流を解析することが、一層困難になる。
【００３４】
（第５の実施の形態）
本発明の第５の実施の形態は、ブリーダ回路に流す電流を、実消費電流に応じて減少させるＩＣカードである。
【００３５】
図６は、本発明の第５の実施の形態におけるＩＣカードの電源電流制御回路24に相当する回路を示す詳細図である。図１の構成と同じ構成については同一番号を付して、その説明を省略する。図６において、抵抗51は、ＩＣカードロジック部10の消費電流を測定するための抵抗である。オペアンプ52は、ＩＣカードロジック部10の消費電流に応じた電圧を発生するアンプである。抵抗53は、ブリーダ回路の電流を制御するためのベース抵抗である。乱数発生回路41は、サブＣＰＵで構成してもよい。
【００３６】
上記のように構成された本発明の第５の実施の形態におけるＩＣカードの動作を説明する。ＩＣカードロジック部10の消費電流に応じた電流を、ブリーダ回路に流す電流から差し引くことで、消費電流の変化を少なくする。外部電源23より、接触コネクタ22を経由し、電源電流制御回路24を通って、ＩＣカードロジック部10へ電源が供給される。
【００３７】
ＩＣカードロジック部10で消費される電流が少ないことを、オペアンプ52で検出し、トランジスタ32の状態をON方向に遷移させる。それにより、抵抗31を通るダミー電流が増加する。ＩＣカードロジック部10で消費される電流が多いことを、オペアンプ52で検出すると、トランジスタ32の状態をOFF方向に遷移させる。それにより、抵抗31に流れるダミー電流が減少する。
【００３８】

抵抗31を流れるダミー電流が、ＩＣカードロジック部10での消費電流を補償するように、抵抗33、オペアンプ52、抵抗51、抵抗53の値を設定しておく。そのため、ＩＣカードロジック部10での消費電流が変化しても、全消費電流の平均値はほぼ一定に保たれる。ＩＣカードロジック部10のみかけの消費電流を一定に保つという機能と、乱数発生回路によるダミー電流を流す機能により、電流解析が難しくなり、セキュリティ確保が可能となる。

【００３９】

上記のように、本発明の第５の実施の形態では、ＩＣカードを、プリーダ回路に流す電流を、実消費電流に応じて減少させる構成としたので、平均消費電流をほぼ一定にすることができる。

【００４０】

【発明の効果】

以上の説明から明らかなように、本発明では、外部から電源を供給する接触式のＩＣカードに、乱数発生器と、乱数発生器で発生した乱数に基づいて電流を流すプリーダ回路とを具備する構成としたので、乱数発生回路による電流のために、処理速度を遅くすることなく、実際の電源電流の変化による解析を困難にして、ＩＣカードの機密を保護することができるという効果が得られる。

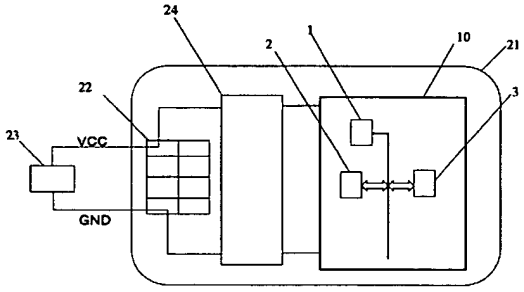
【図面の簡単な説明】

【図１】本発明の第１の実施の形態におけるＩＣカードの概念図、
【図２】本発明の第１の実施の形態におけるＩＣカードの電源電流制御回路図、
【図３】本発明の第２の実施の形態におけるＩＣカードの電源電流制御回路図、
【図４】本発明の第３の実施の形態におけるＩＣカードの電源電流制御回路図、
【図５】本発明の第４の実施の形態におけるＩＣカードの電源電流制御回路図、
【図６】本発明の第５の実施の形態におけるＩＣカードの電源電流制御回路図、
【図７】従来の偽電流発生回路を有するＩＣカードの機能ブロック図、
【図８】従来の電流補償回路を有するＩＣカードの機能ブロック図である。

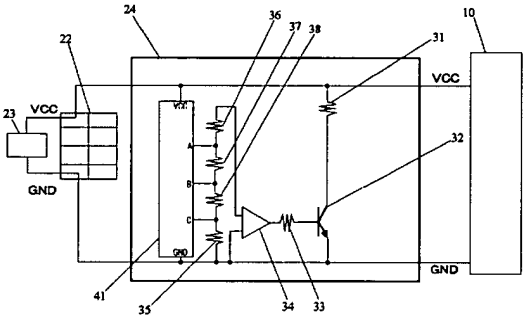
【符号の説明】

1　ＣＰＵ
2　ＲＯＭ
3　ＲＡＭ
10　ＩＣカードロジック部
11　第１出力ポート
12　第２出力ポート
13　第３出力ポート
14　第４出力ポート
21　ＩＣカード
22　接触コネクタ
23　外部電源
24　電源電流制御回路
31,33,35,36　抵抗
37,38,51,53　抵抗
32　トランジスタ
34,52　オペアンプ
41　乱数発生回路
61　サブＣＰＵ
70　乱数発生回路
71　偽電流発生回路
80　半導体集積回路装置
81　主回路部
82　動作電流検出回路部
83　電流補償回路部

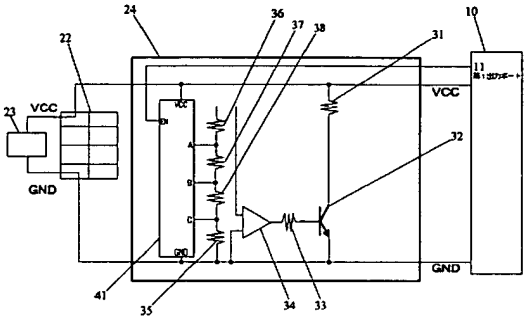
【図１】



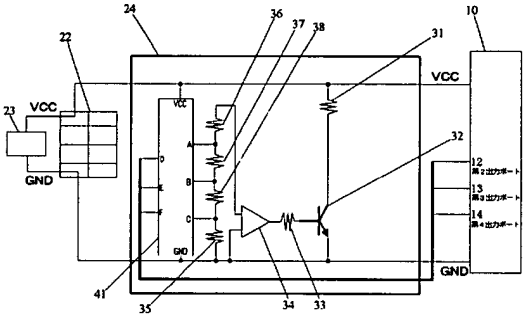
【図２】



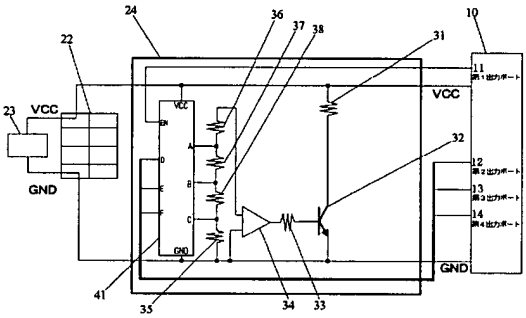
【図３】



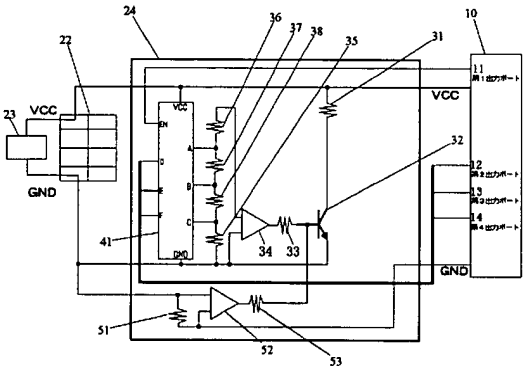
【図４】



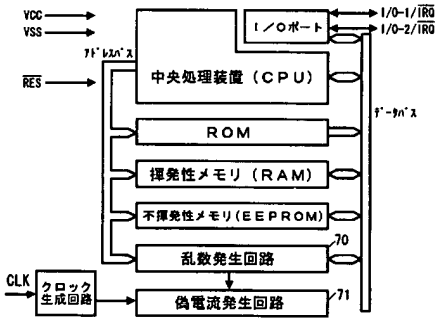
【図５】



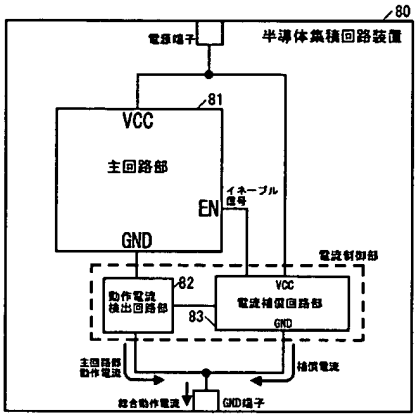
【図６】



【図７】



【図８】


80
電源端子
半導体集積回路装置
81
VCC
主回路部
イネーブル信号
EN
GND
電流制御部
82
動作電流検出回路部
83
VCC
電流補償回路部
GND
主回路部動作電流
補償電流
総合動作電流
GND端子

フロントページの続き

Fターム(参考) 5B035 BB09 CA08 CA11 CA12 CA22 CA38